

WHAT IS CLAIMED IS:

1                   1.     A rights management architecture for securely delivering content to  
2 authorized consumers, the architecture comprising:  
3                   a content provider;  
4                   a consumer system for requesting content from the content provider;  
5                   the content provider generating a session rights object for accessing the  
6 content;  
7                   a KDC (key distribution center) for providing authorization data to the  
8 consumer system, the authorization data for accessing the content;  
9                   a caching server for comparing information in the session rights object with  
10 the authorization data; and  
11                   the caching server forwarding the requested content to the consumer system if  
12 the information matches the authorization data.

1                   2.     The architecture of claim 1 wherein  
2                   the consumer system is redirected to the caching server to receive the  
3 requested content.

1                   3.     The architecture of claim 1 wherein the caching server and the content  
2 provider are combined into a single system identified .

1                   4.     The architecture of claim 1 wherein  
2                   the caching server employs real time streaming for securely forwarding the  
3 encrypted content.

1                   5.     The architecture of claim 1 wherein  
2                   the requested content is encrypted for forwarding to the consumer system.

1                   6.     The architecture of claim 4 wherein  
2                   the caching server and the consumer system exchange control messages for  
3 supporting transfer of the requested content.

1                   7.     The architecture of claim 6 wherein the control messages are encrypted  
2 and authenticated.

1                   8.     The architecture of claim 5 wherein  
2                   the caching server comprises one or more cache disks for storing encrypted  
3 content.

1           9.     The architecture of claim 5 wherein  
2           the KDC distributes cryptographic keys, the KDC employing a blend of  
3 symmetric and public algorithms for distributing the cryptographic keys.

1           10.    The architecture of claim 5 further comprising  
2           a key management protocol for establishing keys between the caching server  
3 and the consumer system.

1           11.    The architecture of claim 10 wherein the key management protocol  
2 comprises  
3           a key request message for requesting a session key from the caching server  
4 and  
5           responsive thereof, a key reply message for providing the session key to the  
6 consumer system.

1           12.    The architecture of claim 11 wherein  
2           the session rights object and the authorization data are included in the key  
3 request message;  
4           wherein the caching server compares information in the session rights object  
5 to the authorization data; and  
6           if the information matches the authorization data, the session key being  
7 provided to the consumer system.

1           13.    The architecture of claim 12 wherein  
2           the content provider generates the session rights object specifying the user's  
3 access privileges for the content.

1           14.    A rights management method for securely delivering content upon  
2 request from a caching server, the method comprising:  
3           providing a content provider communicably coupled to the a caching server;  
4           providing a key management protocol comprising the steps of,  
5           forwarding a ticket challenge message from the caching server to the content  
6 provider, the challenge message for initiating key management;  
7           responsive thereof, sending a key request message from the content provider  
8 to the caching server;  
9           responsive thereof, sending a key reply message from the caching server to the  
10 content provider;  
11           responsive thereof, sending a security established message from the content  
12 provider to the caching server; and

responsive thereof, sending a security established message from the content provider to the caching server; and  
establishing a set of keys for securely delivering content from the content provider to the caching server.

15. The method of claim 14 further comprising  
providing a consumer system for streaming content from the caching server.

16. The method of claim 14 further comprising  
providing a key distribution center for establishing trust between the caching server and the content provider.

17. A rights management method for securely pre-positioning content at a caching server, the method comprising:  
providing a content provider communicably coupled to the a caching server;  
providing a key management protocol comprising the steps of,  
forwarding a key request message from the content provider to the caching server, the key request message for initiating key management;  
responsive thereof, sending a key reply message from the caching server to the content provider; and  
establishing a set of keys for securely delivering content from the content provider to the caching server.

18. The method of claim 17 further comprising  
providing a consumer system for streaming content from the caching server.

19. The method of claim 17 further comprising  
providing a key distribution center for establishing trust between the caching server and the content provider.

20. An authentication system allowing an authorized user to stream content from a caching server within a computing network, the system comprising:  
a content provider for providing the content to the caching server for access by the user;  
a key distribution center receiving from the content provider, a first request to access the caching server, and if authenticated the content provider delivers the content to the caching server; and

8 the key distribution center receiving from the user, a second request to access  
9 the caching server, and if authenticated the user is allowed to stream the content from the  
10 caching server.

1 21. The authentication system of claim 20 wherein the second request is  
2 for a caching server ticket to access the caching server.

1 22. A protocol for securing data transfer between components of a  
2 communication network:

3 a) providing a central server having a database;

4 b) publishing content metadata from a content provider to the central server;

5 c) providing a billing center server, communicably coupled to the central  
6 server;

7 d) reporting billing information from a caching server to the billing center  
8 server;

9 e) providing a provisioning database, coupled to the central server;

10 f) updating the provisioning database with consumer information; and

11 g) using a key management protocol to securely transfer data during any one  
12 or more of step b), step d), and step f).

1 23. The protocol of claim 22 wherein

2 the key management protocol comprises

3 forwarding a key request message for requesting a session key; and

4 receiving a key reply message for providing a session key.